UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/760,592	01/20/2004	Scott N. Gerard	ROC920030316US1	1109

30206 7590 09/26/2007

IBM CORPORATION
ROCHESTER IP LAW DEPT. 917
3605 HIGHWAY 52 NORTH
ROCHESTER, MN 55901-7829

EXAMINER	
BAYOU, YONAS A	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
09/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/760,592	GERARD, SCOTT N.	
	Examiner	Art Unit	
	Yonas Bayou	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-8,13-20,22-24 and 29-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-8,13-20,22-24 and 29-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on *01/20/2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's response filed on 03/23/2007.

2. Claims 1-4, 6-8, 13-20, 22-24 and 29-33 are pending.

3. Claims 5, 9-12, 21, 25-28 and 34 are cancelled.

4. Claims 1, 17 and 33 are amended.

5. Applicant's arguments have been fully considered but they are not persuasive.

6. When responding to the Office action, Applicant is advised to clearly point out the patentable novelty the claims present in view of the state of the art disclosed by the reference(s) cited or the objection made. A showing of how the amendments avoid such references or objections must also be present. See 37 C.F.R. 1.111(c).

Response to Arguments

1. Applicant's arguments with respect to claims 1, 17 and 33 have been considered but are moot in view of the new ground(s) of rejection.

2. Applicant's arguments, see the remarks, filed 07/23/2007, claim 1 is a combination of claims 5, 9, 10, 11, 12 and 26.

NEW GROUND(S) OF REJECTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-4, 6-8, 13-20, 22-24 and 29-33 are rejected under 35 U.S.C. 103(a) as being obvious over Jakobsson et al. Patent No. 6,950,937 in view of Elbe et al. WO 02/48857 A2.

Referring to claims 1, 17 and 33, Jakobsson teaches an apparatus, program code and a method of initiating performance of a computation on at least one untrusted computer, the method comprising:

partitioning the computation into a plurality of computational units that are combinable to generate a result for the computation **[column 2, lines 5-24; column 4, lines 10-20 and fig. 1]**, wherein the computation includes a plurality of arguments, wherein partitioning the computation into the plurality of computational units comprises partitioning using the Chinese Remainder Theorem (CRT) **[column 4, lines 56-67** instead of referring to Chinese Remainder Theorem (CRT), Jakobsson teaches Digital Signature Algorithm], wherein partitioning the computation into the plurality of computational units comprises selecting a plurality of relatively prime moduli and generating each computational unit by performing a modulo operation on each of the

plurality of arguments using one of the plurality of relatively prime moduli **[column 1, lines 14-28 and column 5, lines 1-17]**, and wherein selecting the plurality of relatively prime moduli includes selecting each modulus from a superset of relatively prime moduli **[column 5, lines 1- 17]**;

partitioning a plurality of computations into multiple computational units using different sets of moduli selected from the superset of relatively prime moduli **[column 5, lines 1- 17]**;

initiating execution of both the at least one distractive computational unit and computational units from multiple computations on the untrusted computer to inhibit reconstitution of the computations by an untrusted party **[column 2, lines 12-16; column 3, lines 15- 52; column 4, lines 20-48 and figs. 1-3;** instead of referring to partitioning the computation into a plurality of computational units, generating at least one distractive computational unit and initiating execution of both computations on the untrusted computer, Jakobsson teaches division of the process into task transformation (partitioning of computation) which contains replication, dependency, blinding and random computation, such that replication, dependency and random permutation operation corresponds to a plurality of computational units where as blinding operation corresponds to one distractive computational unit and also result transformation corresponds to initiating execution of computations];

receiving result data generated during execution of the computational units from the multiple computations **[column 2, lines 5-24; column 4, lines 10-20 and fig. 1]**;

and

generating results for the multiple computations from the result data **[column 2, lines 5-24; column 4, lines 10-20 and fig. 1].**

Jakobsson does not appear to explicitly teach generating at least one distractive computational unit, wherein the distractive computational unit comprises a dummy computational unit. However, Elbe teaches that one type of cryto coprocessors performs "dummy" computation for the purpose of making harder for an attacker to find out parameters of the "useful" crypto coprocessor algorithm **[page 3, paragraph 0023; page 4, paragraph 0047 and 0049].**

Referring to claims 2 and 18, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, wherein the distractive computational unit comprises a computational unit generated from partitioning a second computation **[column 2, lines 12-16; column 4, lines 20-55 and figs. 3-7].**

Referring to claims 3 and 19, Jakobsson teaches a method which inherently teach the program code as applied above. Furthermore, Jakobsson teaches a method, wherein initiating execution of both the at least one distractive computational unit and at least one of the plurality of computational units includes interleaving the at least one distractive computational unit among multiple computational units from the plurality of computational units **[column 5, lines 17-58 and fig. 3].**

Referring to claims 4 and 20, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, wherein partitioning the computation uses a different algorithm than that used to partition the second computation **[column 4, lines 56-67].**

Referring to claims 6 and 22, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, wherein the distractive computational unit comprises a computational unit generated from a second partitioning of the computation **[column 2, lines 12-16; column 5, lines 17-column 7, lines 51 and fig. 3].**

Referring to claims 7 and 23, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, further comprising initiating execution of at least one of the plurality of computational units on a second computer **[column 3, lines 30-45].**

Referring to claims 8 and 24, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, further comprising initiating execution of all of the plurality of computational units on the untrusted computer **[column 3, lines 30-45; column 3, lines 52-57 and fig. 1].**

Referring to claims 13 and 29, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, wherein the untrusted computer is coupled to a grid computing network **[column 3, lines 1-17 and fig. 1].**

Referring to claims 14 and 30, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, wherein partitioning the computation is performed by a client computer coupled to the grid computing network **[column 3, lines 35-41].**

Referring to claims 15 and 31, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, wherein partitioning the computation is performed by a broker computer coupled to the grid computing network, the method further comprising receiving the computation from a client computer **[column 4, lines 20-31; fig. 1 and fig. 3].**

Referring to claims 16 and 32, Jakobsson teaches a method as applied above. Furthermore, Jakobsson teaches a method, wherein partitioning the computation, generating the distractive computational unit, and initiating execution of both the distractive computational unit and the one of the plurality of computational units on the untrusted computer are performed by at least one computer coupled to the untrusted computer, the method further comprising

communicating the distractive computational unit and the one of the plurality of computational units to the untrusted computer **[column 2, lines 1-16; column 5, lines 17-colunm 7, line 51; fig. 1 and fig. 3].**

Jakobsson and Elbe are analogous art because both teach useful computational algorithms.

Accordingly, it would have been obvious to one having ordinary skill in the art at the time of the invention to modify the method of Jakobsson to incorporate the "dummy" computation of Elbe because the processor type performing dummy computations is selected advantageously in random manner, so that an attacker, will never know which processor type carries out useful computations.

Conclusion

3. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yonas Bayou whose telephone number is 571-272-7610. The examiner can normally be reached on m-f,7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571-272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

Yonas Bayou

YB